acreq
Association de cadres retraités de l'éducation du Québec

Politique concernant la protection des renseignements personnels

Adoptée à l'Assemblée générale annuelle
Tenue le 12 juin 2024

Résolution AG-20240612-226

Préambule

Les lois encadrant la protection des renseignements personnels

Dans le cadre de l'exercice de leurs fonctions, les administrateurs élus au Conseil d'administration de **l'Association de cadres retraités de l'éducation du Québec (ACREQ),** les présidences de section, les membres élus des conseils de section de même que le personnel administratif traitent des renseignements personnels relatifs aux membres de l'Association et aux personnes qui sont à leur emploi, le cas échéant.

L'un des droits fondamentaux proclamé par la *Charte des droits et libertés de la personne* est celui du **respect de la vie privée**. Ainsi, chaque personne a le droit de contrôler l'accès et le partage des renseignements qui la concernent.

Dans le but d'assurer le respect de ce droit fondamental, les lois imposent plusieurs règles relatives au traitement des renseignements personnels dont les entreprises et les associations sans but lucratif peuvent avoir la garde ou le contrôle.

C'est le cas de la *Loi sur la protection des renseignements personnels dans le secteur privé*, laquelle prévoit certaines obligations incombant spécifiquement aux entreprises et aux associations sans but lucratif en matière de protection des renseignements personnels.

Notons qu'une entreprise ou une association à but non lucratif qui ne respecte pas ces règles peut s'exposer à de sévères sanctions.

NOUVELLES OBLIGATIONS

Adoptée par l'Assemblée nationale en 2021, la ***Loi modernisant des dispositions législatives en matière de protection des renseignements personnels***, dont la plupart des dispositions sont entrées en vigueur le **22 septembre 2023**, est venue moderniser la ***Loi sur le secteur privé*** pour l'adapter aux plus récents développements technologiques et aux autres tendances qui caractérisent la société d'aujourd'hui. Cette loi accorde plus de droits aux individus et impose de nouvelles obligations aux entreprises et aux associations sans but lucratif. **Les administrateurs, les membres des conseils de section et le personnel de l'ACREQ doivent adapter leurs pratiques internes afin de se conformer à cette nouvelle réglementation.**

Les lois s'appliquent peu importe le contexte dans lequel les renseignements personnels sont recueillis, détenus, utilisés, communiqués ou conservés dans le cadre des activités de l'Association. Que ce soit lors de la sollicitation de futurs retraités, de l'adhésion de nouveaux membres, de la communication des informations concernant un membre, les administrateurs, les membres des conseils de section et le personnel de l'ACREQ doivent assurer la protection des renseignements personnels qu'ils détiennent.

1. Définitions

1.1 Renseignements personnels

Un **renseignement personnel** est un renseignement qui concerne une **personne physique** et qui permet de **l'identifier**, **directement ou indirectement.**

Il s'agit d'un renseignement permettant de faire connaître quelque chose de quelqu'un, d'avoir un rapport avec une personne physique et d'être susceptible de distinguer cette personne par rapport à quelqu'un d'autre.

Un renseignement personnel peut être détenu sur **différents supports** : un écrit (document papier, courriel, texto), un support sonore (enregistrement d'une conversation, message vocal), un support visuel (photo, vidéo).

Voici quelques exemples de renseignements personnels que l'ACREQ peut être appelée à recueillir :

- Les renseignements d'identité : date de naissance, âge, sexe, numéro d'assurance sociale (NAS);
- Les coordonnées : adresse postale personnelle, adresse électronique, numéro de téléphone;
- Photo de la personne, seule ou en groupe;
- Etc.

1.2 Renseignements personnels sensibles

Certains renseignements personnels concernent des zones de la vie privée que la plupart des gens ne souhaitent pas révéler au grand public; ils sont qualifiés de « renseignements personnels sensibles ». En fonction du contexte, il peut s'agir, entre autres, de renseignements médicaux, d'opinions politiques, de croyances religieuses, etc.

Ce sont aussi des renseignements dont la divulgation accroît les risques **d'usurpation d'identité** : le numéro d'assurance sociale, les renseignements sur des cartes de crédit, la date de naissance, etc**.**

Les renseignements sensibles doivent faire l'objet d'une attention accrue à toutes les étapes de la gestion des renseignements personnels.

Les renseignements personnels typiquement détenus par l'Association sont de nature sensible, puisqu'ils sont reliés à la situation personnelle.

2. Rôle et responsabilités du Conseil d'administration

La modernisation de la *Loi sur le secteur privé* prévoit que toute personne qui exploite une entreprise incluant les associations sans but lucratif, est responsable de la protection des renseignements personnels qu'elle détient.

Ainsi, la personne ayant la plus haute autorité au sein de l'Association sera d'office responsable de la protection des renseignements personnels au sein de son entreprise. Elle pourra toutefois déléguer cette fonction à un tiers. Cette personne doit posséder les compétences requises et doit bénéficier des pouvoirs décisionnels en lien avec ses fonctions.

Le titre et les coordonnées du responsable de la protection des renseignements personnels doivent être publiés sur le site Internet de l'Association.

C'est l'Association et son Conseil d'administration qui « détiennent » juridiquement les renseignements personnels. Bien qu'ils puissent conserver une copie des renseignements dans le cadre de leur mandat, les administrateurs, les membres des conseils de section et le personnel doivent détruire les documents avec diligence lorsque les renseignements ne sont plus nécessaires.

L'Association doit fournir des directives et des politiques claires et conformes aux lois en matière de protection des renseignements personnels. Depuis septembre 2022, elle doit tenir un **registre des incidents de confidentialité** et **déclarer** à la Commission d'accès à l'information tout incident de confidentialité impliquant un renseignement personnel présentant un risque sérieux de préjudice.

3. Confidentialité des renseignements personnels et principe de consentement

3.1 Principes essentiels dans la réglementation

Conformément au respect du droit à la vie privée, deux principes essentiels ressortent de la réglementation et doivent être respectés :

- La **confidentialité** par défaut des renseignements personnels;
- La nécessité d'un **consentement** de la personne visée pour la cueillette, l'utilisation, la communication et la conservation des renseignements personnels, à moins d'une exception prévue expressément par la loi.

3.2 Exception : renseignements personnels ayant un caractère public

En vertu des exceptions prévues par les différentes lois, certains renseignements, bien qu'ils soient personnels, demeurent publiquement accessibles. En effet, toute personne peut consulter des registres publics dont certains contiennent des renseignements personnels, tel le Registre des entreprises du Québec.

Cependant, un renseignement public complété par un renseignement qui ne l'est pas doit demeurer confidentiel. Par exemple, l'information concernant les coordonnées d'un administrateur saisies au Registre des entreprises du Québec jumelée à sa date de naissance sont des renseignements personnels confidentiels.

3.3 Consentement valide

À toutes les étapes de traitement d'un renseignement personnel, il y a lieu de demander le consentement de la personne concernée, à l'exception des cas prévus spécifiquement dans la loi.

3.3.1 Consentement manifeste, libre et éclairé

Le consentement doit être clair et sans équivoque. La personne concernée doit être consciente des raisons pour lesquelles on recueille ses renseignements et de l'utilisation qui en sera faite. Il est important que le consentement soit manifesté de façon expresse.

3.3.2 Consentement donné à des fins spécifiques et limité dans le temps, en termes simples et clairs

Le consentement doit être limité aux fins pour lesquelles il a été donné et il ne vaut que pour la durée nécessaire à la réalisation de ces fins, soit la durée de l'adhésion à l'Association.

NOTE : Afin d'assurer la validité d'un consentement, il est important de préciser, de la façon la plus concrète possible, les fins pour lesquelles les renseignements sont recueillis et communiqués à des tiers, le cas échéant.

Au moment de la cueillette initiale des renseignements personnels, si l'Association sait qu'elle utilisera ces renseignements à d'autres fins, elle doit tout de suite demander à la personne concernée, l'autorisation pour une utilisation secondaire. C'est le cas, par exemple, pour l'envoi de convocations, d'invitations, de bulletins d'information, de communiqués, des cartes de Noël ou d'anniversaire. Il est alors recommandé de procéder par écrit par le biais du formulaire d'adhésion ou de consentement, le cas échéant.

Comme pour la cueillette initiale des renseignements, toutes les conditions suivantes doivent être respectées pour que le consentement soit valide.

Conditions de validité d'un consentement à la cueillette des renseignements personnels :

- Lorsque faite par écrit, la demande de consentement doit être présentée distinctement de toute autre information communiquée à la personne concernée;
- Le consentement doit être demandé à chacune des fins pour lesquelles les renseignements sont recueillis;
- Le consentement doit être rédigé en termes simples et clairs, et doit contenir des informations spécifiques;
- Le consentement ne vaut que pour la durée nécessaire à la réalisation des fins auxquelles il a été demandé;
- À la demande de la personne concernée, l'Association devra lui prêter assistance pour s'assurer qu'elle comprenne la portée du consentement demandé.

4. Cueillette des renseignements personnels

L'Association est appelée à recueillir les renseignements personnels dans plusieurs situations :

- Lors de la réception par la poste ou par voie électronique du formulaire d'adhésion de personnes retraitées qui souhaitent devenir membre de l'ACREQ;
- Par les administrateurs, les membres des conseils de section ou le personnel lors d'appel téléphonique, de réception de courriels ou de courrier postal d'un membre annonçant des modifications à ses coordonnées;
- En prenant des notes manuscrites ou sur ordinateur ou en faisant appel à un logiciel d'enregistrement des données;
- Etc.

Pour toute situation, elle doit toujours s'assurer qu'aucune autre personne ne puisse entendre ou voir ses informations avec le membre lors de la cueillette des renseignements personnels.

4.1 Principes à respecter

L'Association doit respecter les principes suivants lorsqu'elle recueille des renseignements personnels.

- **Déterminer préalablement les fins de la cueillette des renseignements personnels.**
- Seuls les renseignements personnels **nécessaires, c'est-à-dire *indispensables* et non simplement *utiles*,** peuvent être recueillis.
- Recueillir les renseignements personnels par **des moyens licites** (légaux).

4.2 Devoir d'information lors de la cueillette des renseignements personnels

Conformément au principe de transparence, l'Association doit informer la personne concernée des informations décrites ci-dessous et prescrites par la loi. Il est fortement recommandé de procéder par écrit.

4.2.1 Informations obligatoires

Ces informations doivent figurer sur le formulaire de consentement écrit que l'Association fera signer :

- **les fins** pour lesquelles on doit recueillir les renseignements personnels;

- **le nom des tiers pour qui la collecte est faite** : Revenu Québec, l'Association représentée par le Conseil d'administration et un conseil de section;

- **le droit de retirer son consentement**;

  La personne doit être informée de son droit de retirer à tout moment son consentement à la cueillette des renseignements personnels.

- **le droit d'accès et de rectification**.

  La personne doit être informée qu'elle a le droit d'avoir accès à ses renseignements personnels détenus par l'Association et de faire rectifier un renseignement inexact, incomplet ou équivoque, ou si sa collecte, sa communication ou sa conservation n'est pas autorisée par la loi. Pour ce faire, cette

personne peut adresser une demande à l'attention du Responsable de la protection des renseignements personnels de l'Association.

4.2.2 Informations facultatives

Les informations suivantes devront être communiquées à la personne **qui le demande** :

- La **durée de conservation** des renseignements personnels;
- Les **coordonnées du responsable** de la protection des renseignements personnels au sein de l'Association;
- La **nature des renseignements** personnels recueillis;
- Les **catégories de personnes** qui pourront avoir accès à ses renseignements au sein de l'Association.

4.2.3 Informations sur les témoins de connexion (*cookies*)

Un témoin de connexion (ou *cookie*) est un fichier texte déposé par un serveur sur un appareil (un ordinateur ou un appareil mobile) lorsqu'une personne consulte un site Internet.

La cueillette des renseignements personnels au moyen des témoins de connexion doit être balisée dans la **politique de confidentialité** que les associations doivent mettre en place.

Aussi, lorsqu'une personne visite le site Internet de l'Association, un bandeau « cookies » devra apparaître (un « pop-up ») permettant à la personne de gérer les témoins de connexion et d'activer éventuellement les fonctions permettant le profilage aux fins publicitaires. Attention **:** lorsqu'un témoin de connexion permet l'identification d'une personne, la localisation géographique ou le profilage, notamment, aux fins publicitaires, il doit être désactivé par défaut.

4.3 Formule de consentement

Pour récapituler les informations données ci-dessus, voici les éléments obligatoires que doit contenir une formule de consentement à la cueillette des renseignements personnels :

- Chacune des fins pour lesquelles les renseignements sont recueillis;
- Les moyens de cueillette des renseignements (par exemple, par le biais d'un formulaire de consentement écrit);
- L'utilisation qui sera faite des renseignements recueillis (l'utilisation doit correspondre aux fins pour lesquelles les renseignements sont recueillis);
- Le cas échéant, l'identité des personnes ou des entreprises pour lesquelles la cueillette sera faite;
- Les noms ou les catégories des tiers auxquels il sera nécessaire de communiquer les renseignements;
- Précision que le renseignement ne vaut que pour la durée de la réalisation des fins pour lesquelles il a été recueilli. Dans la mesure du possible, il faut indiquer la période de validité de consentement (déterminée ou déterminable).

5. Utilisation des renseignements personnels

Les renseignements personnels ne peuvent être utilisés qu'aux fins pour lesquelles ils ont été recueillis.

Lorsque le membre ne renouvelle pas son adhésion ou décède, l'Association **ne doit plus** utiliser les renseignements personnels qu'elle possède.

5.1 Exceptions : utilisation sans le consentement

La loi prévoit des cas d'exception quand les renseignements personnels peuvent être utilisés sans le consentement de la personne concernée :

- L'utilisation secondaire est compatible avec les fins pour lesquelles le renseignement a été initialement recueilli. Il doit y avoir un lien direct et pertinent avec les fins initiales.
- L'utilisation est manifestement au bénéfice de la personne concernée.
- L'utilisation est nécessaire à des fins d'étude, de recherche ou de production de statistiques, mais les renseignements doivent être dépersonnalisés de façon à empêcher d'identifier directement la personne concernée.

5.2 Mesures de sécurité lors de l'utilisation des renseignements

L'Association est tenue de prendre des mesures de sécurité raisonnables pour assurer la protection des renseignements personnels qu'elle détient. Ces mesures doivent notamment tenir compte de la **sensibilité** des renseignements, de la **finalité** de leur utilisation, de leur **quantité**, de leur **répartition** et de leur **support**.

Dans le cadre des mesures de sécurité, il y a lieu notamment de **restreindre l'accès** physique et informatique aux renseignements aux seules personnes auxquelles il est nécessaire d'y accéder dans le cadre de leur fonction.

L'Association doit s'assurer que le **support** choisi pour détenir et utiliser les renseignements personnels est stable, sécuritaire et qu'il assure la confidentialité en tout temps.

5.2.1 Incident de confidentialité

Dans la foulée de fuites possibles de renseignements personnels et dans le contexte de la convergence massive vers le télétravail, la nouvelle loi a mis clairement l'accent sur la **cybersécurité**.

Un **incident de confidentialité** est défini comme un événement susceptible de compromettre la confidentialité des renseignements personnels lorsqu'ils sont utilisés par une entreprise, soit :

- l'accès non autorisé par la loi à un renseignement personnel;
- l'utilisation non autorisée par la loi d'un renseignement personnel;
- la communication non autorisée par la loi d'un renseignement personnel;
- la perte d'un renseignement personnel ou toute autre atteinte à sa protection.

Peuvent constituer un incident de confidentialité des événements comme le vol, la fraude, la perte (causée par un virus ou une faille informatique, une fuite, une attaque informatique, une erreur), une action délibérée (l'extraction de renseignements par un employé ou une personne non autorisée), etc.

Si un incident se produit et présente un risque sérieux de préjudice, l'Association doit le **dénoncer** avec diligence aux **personnes concernées** ainsi qu'à la **Commission d'accès à l'information** (CAI). Elle pourra, à sa discrétion, aviser aussi toute entité susceptible de diminuer le risque en ne lui communiquant que les renseignements nécessaires à cette fin, et ce, sans le consentement de la personne concernée (par exemple, la police, son fournisseur informatique, etc.).

Pour **évaluer le risque** qu'un préjudice soit causé à une personne dont un renseignement personnel est impliqué dans un incident de confidentialité, il faudra considérer notamment la sensibilité du renseignement concerné, les conséquences appréhendées de son utilisation et la probabilité qu'il soit utilisé à des fins préjudiciables. Dans le cas d'un accès non autorisé aux renseignements dont la divulgation accroît les risques d'usurpation d'identité, on doit considérer que le risque est sérieux et le dénoncer.

Comme l'ensemble des entreprises du Québec, l'Association doit **prendre des mesures visant à diminuer les risques de préjudice** en cas d'incident de confidentialité.

Afin de minimiser le préjudice possible, il est fortement recommandé de mettre en place des mesures préventives en matière de cybersécurité (revue des systèmes informatiques, formation du personnel, politiques de contrôle internes) ainsi que des **mesures de gestion des incidents**.

Notamment, il est recommandé d'établir un protocole de gestion d'un incident de confidentialité dans lequel seront identifiés les membres d'une cellule de crise qui auront la charge de gérer l'incident et de déterminer les actions concrètes à poser après l'incident. Il est également recommandé de se munir d'une assurance couvrant les cyber-risques.

De plus, l'Association devra tenir un **registre des incidents de confidentialité.**

L'obligation de gestion et de dénonciation des incidents de confidentialité doit être prise au sérieux compte tenu des sanctions administratives sévères qui pourraient être imposées par la CAI en cas de non-respect des nouvelles règles.

6. Communication des renseignements personnels

6.1 Consentement à la communication

Le principe de consentement s'applique en matière de communication des renseignements personnels à des tiers. Une personne qui consent conformément à la loi à fournir ses renseignements personnels est présumée consentir à leur communication aux fins pour lesquelles ils ont été recueillis.

Ce n'est qu'exceptionnellement qu'un renseignement peut être communiqué sans le consentement de la personne concernée, c'est-à-dire, lorsque :

- une telle situation est prévue expressément dans la loi;
- un renseignement personnel a un caractère public en vertu de la loi.

6.2 Liste des personnes et entités

L'Association peut être appelée à communiquer les renseignements personnels à différentes personnes et entités, par exemple à :

- Retraite-Québec pour le prélèvement de la cotisation mensuelle directement à la source de sa rente de retraite;
- aux administrateurs du Conseil d'administration;
- à la présidence de sa section ou ses représentants;
- au personnel de l'ACREQ.

7. Conservation des renseignements personnels

Lorsque les fins pour lesquelles un renseignement personnel a été recueilli ou utilisé sont accomplies, l'Association doit le détruire, sous réserve d'un délai de conservation prévu par une loi.

Ainsi, le règlement de **conservation des renseignements personnels** prévoit spécifiquement que l'Association doit conserver les registres et les dossiers pendant au moins 6 ans suivant leur fermeture définitive. Ces renseignements peuvent être sous forme électronique (dans le téléphone cellulaire (textos, courriels), dans l'ordinateur, sur une tablette, dans le cloud) ou sous forme papier (dossiers, livres et registres).

7.1 Destruction sécuritaire

Aux fins de conformité de la destruction, l'Association doit prendre les mesures de sécurité nécessaires pour protéger le caractère confidentiel des renseignements qui s'y trouvent.

À cet effet, l'Association doit :

- Sécuriser les documents en attente de destruction;
- S'assurer que la destruction des dossiers et des registres ne soit confiée qu'à quelques personnes spécifiquement désignées et qu'elle soit effectuée conformément à une procédure clairement définie et dans des conditions précises;
- S'assurer que la méthode de destruction soit adaptée au support et au niveau de confidentialité des documents et que le contenu soit détruit de façon définitive;
- S'assurer de ne jamais laisser la version papier de documents contenant des renseignements personnels dans des bacs de recyclage sans avoir procédé préalablement au déchiquetage sécuritaire;

Note :

La Politique concernant la protection des renseignements personnels entrera en vigueur dès son adoption par l'Assemblée générale des membres.